公開鍵暗号危殆化対策のためのリスク評価

佐々木良一

近年，利用が増大しつつあるデジタル署名は，電子の世界のはんこの機能を実現するものであり，その安全性は公開鍵暗号の安全性に依存している．したがって，公開鍵暗号が危殆化した場合のデジタル署名ならびに署名付文書への影響とその対策を検討せざるを得ない．そこで，公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書に関連した各種対策の最適な組合せを対策費用とリスク低減効果のバランスを考慮しつつ求める評価方法を開発した．さらにその方法を適用し，ある想定した状況における最適な対策案の組合せを求めたので，その適用結果を報告する．

キーワード：公開鍵暗号，デジタル署名，暗号の危殆化，リスク評価，リスク分析

1. はじめに

インターネットの発展に伴い，電子政府や，電子商取引などが普及しつつある．これらを安全かつ安心して利用するための基盤技術として電子の世界のはんこの機能を実現するデジタル署名がある（デジタル署名の仕組みについては例えば文献[1]のpp. 116-119などを参照）．デジタル署名は公開鍵暗号の安全性に強く依存しており，公開鍵暗号が安全であれば署名者以外は，署名用秘密鍵を知り得ないという前提の下に利用されている．

しかし，コンピュータの演算能力の向上や新しい攻撃手法の発見などにより，公開鍵暗号が安全であるという前提が崩壊してしまう危険性を無視することはできない．公開鍵暗号の安全性が喪失してしまうことを，「公開鍵暗号の危殆化」と呼ぶ．現実に公開鍵暗号の危殆化が懸念されており，2010年以降に開発するシステムについては，鍵長1024ビットのRSA暗号を使用するのはやめるべきであるという指摘もある[2]．公開鍵暗号が危殆化すると，署名用秘密鍵が知られてしまい，誰もが，その人に成りすまし，署名付き文書を偽造することができるようになってしまう．電子借用書などの不正作成や改ざんが可能になるのである．公開鍵暗号の危殆化以外に，SHA-1等のハッシュ関数の危殆化の可能性についても指摘されているが，ここでは紙面の制約から前者を中心に記述する．

ささき　りょういち
東京電機大学 未来科学部
〒101-8457 千代田区神田錦町2-2

公開鍵暗号やハッシュ関数の危殆化を確認した際に，安全性の高い公開鍵暗号（例えば，鍵長2048ビットのRSA暗号）やハッシュ関数（例えば，SHA-256）を用い新しくデジタル署名付き文書を作成できるようにする移行対策は色々検討され始めている[3]．しかし，すでに存在しているデジタル署名付き文書に対する対策の検討については，非常に限定されており，それも定性的分析にとどまっていた．さらに既存のデジタル署名付き文書に対する対策において対策コストと対策効果のバランスを考慮して評価する手法はなく，対策のスムーズな導入が困難であった．

そこで，公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書の証拠性を確保するために必要な対策の最適な組合せを，費用とリスク低減効果のバランスを考慮しつつ求めることのできるリスク評価方法を開発した[4]．著者らは，個人情報漏洩対策などのために，1つのリスク対策が別のリスクを引き起こす可能性を考慮しつつ，関与者間の合意が得られる対策案の組合せを求めるためのツールである多重リスクコミュニケータ[5]を開発しており，今回提案したのは，これを，公開鍵暗号危殆化対策用に改良したものである．本稿では，この方法とその適用結果の一例を示す．

ここでは，対策の最適な組合せを求める際に必要となるリスク分析手法として原子力工学の分野で実績のあるイベントツリー分析（文献[1]のpp. 88-93など参照）を利用し，さらに，最適化手法として，組合せ最適化手法を用いている．

2. 評価方法

2.1 評価方法の概略

公開鍵暗号の危殆化が発生した際，デジタル署名付き文書へのリスクを軽減するような最適な対策案を求めるリスク評価方法を以下に示す（図1参照）．

(1) 対象の決定と予備的検討

ここでは，分析の対象や分析の前提を明確化し，関与者の抽出，脅威・脆弱性の抽出，対策の予備的抽出などを行う．

(2) イベントツリー分析によるリスク分析

(1)で決定した分析の対象，分析の前提，関与者，脅威・脆弱性などに基づき，イベントツリーを作成する．イベントツリー分析については，2.2節で説明する．

(3) 最適化問題としての定式化

最適解を算出するのに必要である目的関数・制約条件の定式化を行う．(1)でリストアップした各対策案候補を採択するか，しないかを0-1変数で表し，組合せ最適化問題として定式化することを前提とする．この定式化段階において(2)のイベントツリー分析の結果が用いられる．

(4) パラメータ値の決定

(3)の定式化の際に，係数として与えられている対策コスト，確率，影響といったパラメータの値を決定する．あわせて制約条件の値を設定する．

(5) 最適解の求解

設定された制約条件の下で，最適な対策案の組合せを算出する．1つの制約条件値の下ではなく制約条件値を変化させるなどして，様々な状況での最適解を算出する．

(6) 結果の分析

上記の(5)で行った種々の条件下での最適解の求解結果を見直し，定式化方法やパラメータの値，制約条件の値を変更する必要がないかどうか検討を行う．

少数の解析者により，上記の(1)-(6)が一応の結果が得られたら，その結果をいろいろな専門家に見せつつ，合意が得られるまで一緒にこの過程を繰り返す．

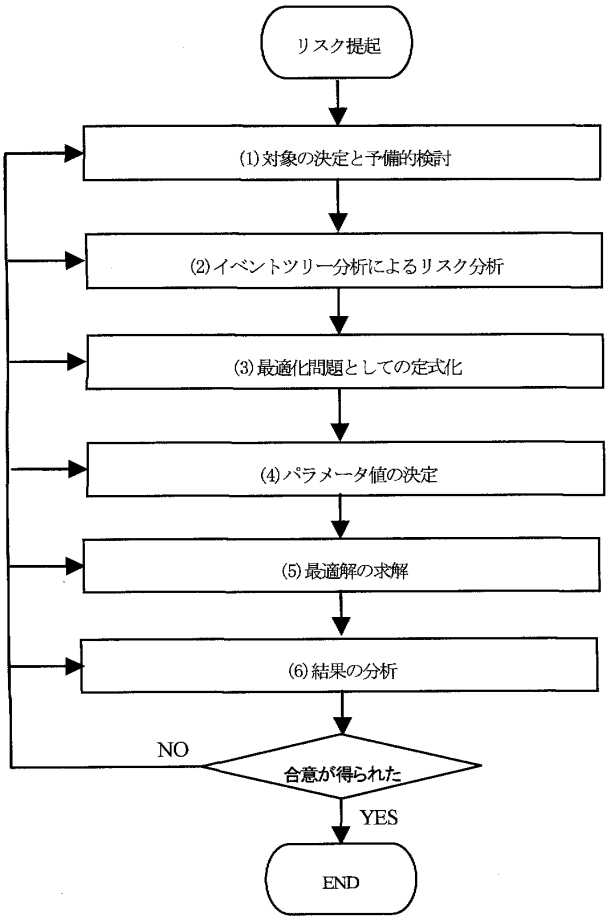


図1 最適な対策案を求める手順のフローチャート

2.2 ETAを用いたリスク分析

ここでは，イベントツリー分析（ETA）を用いて既存の署名付き文書に対してリスク分析を行う方法を説明する．一般的なETAの手順は以下のとおりである．

(a) イベントツリー分析は，事故の引き金になる可能性のある異常事象を初期事象と呼び，これをリストアップする．ここでは，建物の火災の発生を初期事象として考えてみることにしよう（図2参照）．

(b) 初期事象が決定すると，次に，イベントツリーの構造を決定する．ETAでは，初期事象が発生したとき，それを保証する各種の安全対策（ここでは，初期消火と本格消火）をヘッディング項目として図2に示すように記述する．

(c) 次にヘッディング項目に示された各種の安全対策の成否の組合せをシーケンスとして表現する．図2の例では，安全対策として初期消火対策と，本格消火対策とがあり，それぞれの対策の成功，失敗に応じて分岐を行い，全体で3つのシーケンスを得ることができる．ここで，初期消火に成功すれば，本格消火は必要ないので本格消火の部分での分岐はないようになっている．

(d) 統計データやフォルトツリーなどを用い，初期事象の発生頻度（図2ではP_0）や各種安全対策が機能しない確率（図2ではP_1, P_2など）を計算する．これらの確率はどのような対策案を作用するかによって変化する．続いてこれらの値を用い，シーケンス別

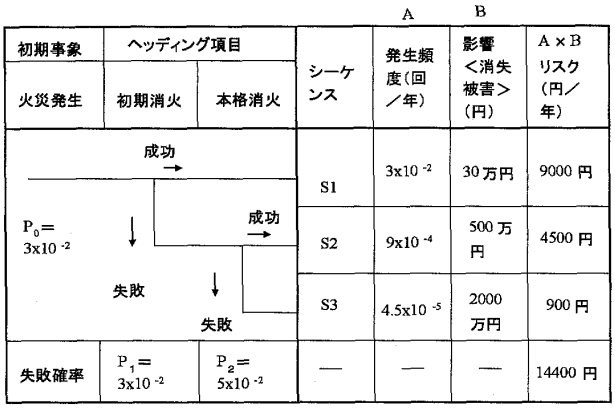


図2　イベントツリーの例

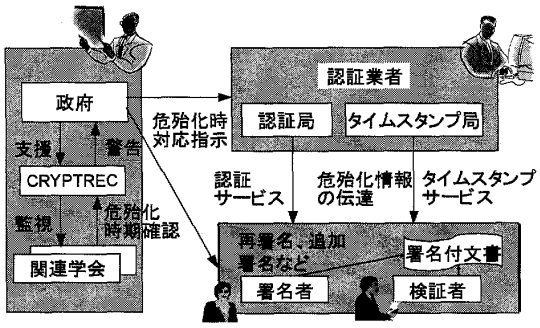


図3　危殆化発見時の対応体制

の発生頻度を計算する．

(e) イベントツリーのシーケンスごとに影響の推定を行う．影響としては死亡者数や平均余命の短縮年や，対策費用などが目的に応じて使い分けられる．図2では，火災が広がることによる損害額を用いている．

(f) 図2のイベントツリーを用い，(d)(e)の結果より，シーケンス別の発生頻度と，リスクを計算する．ここで，各シーケンスのリスクは，発生頻度と影響の大きさとなっている．したがって，そのリスクは，シーケンス1が9000円/年，シーケンス2が4500円/年，シーケンス3が900円/年となっている．そして，各シーケンスのリスクを合計することにより，全体のリスクを，14400円/年であると推定している．

(d) で述べた対策などを0-1変数としてリスクの値を表現することによって，2.1節(3)などの最適化問題としての定式化が可能となる．

3. 公開鍵暗号危殆化対策への適用

図1に沿って説明を行う．

(1) 対象の決定と予備検討

ここでの対象は，公開鍵暗号が危殆化することが明らかになった場合の署名付文書への対策である．そして，リスク評価を行う上で対象とすべき主なエンティティは次の5つである（図3）．

- 政府：暗号の危殆化を監視し，危殆化が発生した場合には認証業者や検証者に伝達する．
- CRYPTREC：Cryptography Research and Evaluation Committeesの略であり，電子政府推奨暗号の安全性を評価・監視し，暗号モジュール評価基準等の策定を検討するプロジェクトである．総務省および経済産業省が共同で開催する暗号技術検討会と，独立行政法人情報通信研究機構（NICT）および独立行政法人情報処理推進機構（IPA）が共同で開催する暗号技術監視委員会および暗号モジュール委員会で構成される．
- 認証業者（認証局，タイムスタンプ局）：認証サービスやタイムスタンプサービスを提供する．危殆化が発生した場合には対策を行い，ユーザに対して危殆化の伝達を行う．
- 署名者：署名付文書を作成し，検証者に送る．
- 検証者：署名付き文書を生成・管理し，デジタル署名の検証を行う．

また，分析の前提は以下のとおりである．

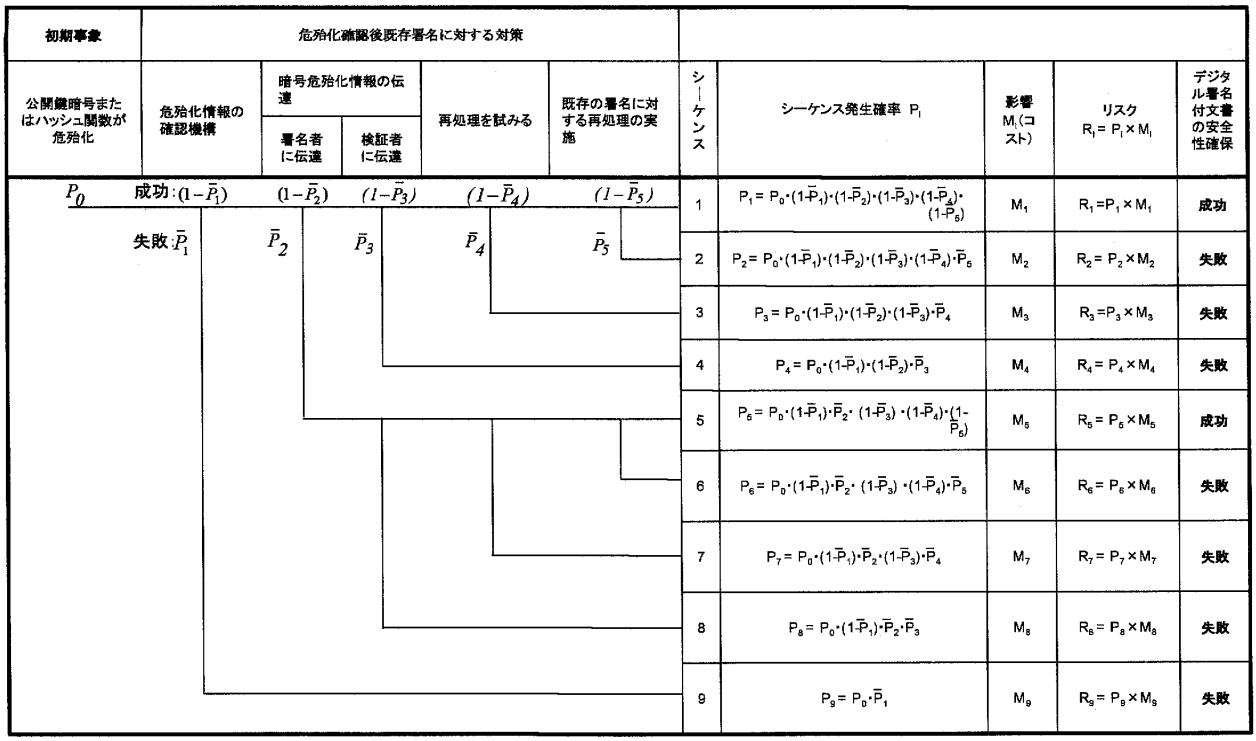
① 公開鍵暗号の危殆化を確認した際に，十分に既存の署名に対して対策がとれる段階で危殆化を発見するものとし，かつ危殆化が発生しても十分に既存の署名の証拠性を確保できる代替公開鍵暗号が存在するものとする．

② 署名に利用する公開鍵暗号はRSAの1024 bit鍵長のものを利用し，公開鍵証明書に使用するものはRSAの2048 bit鍵長のものを利用する．ハッシュ関数はいずれもSHA-1を利用するものとする．

③ 適用モデルとしては，署名者が署名し検証者に渡した電子借用書を対象とし，返済完了前に公開鍵暗号が危殆化してしまうような場合についてリスク分析を行う．

(2) イベントツリー分析によるリスク分析

図4に示すようなイベントツリーを作成した．ここで，ヘッディング項目に対応する対策方法は，(a)危殆化情報の確認，(b)暗号危殆化情報の伝達（署名者に伝達），(c)暗号危殆化情報の伝達（検証者に伝達），(d)署名つき文書の再処理を試みる，(e)既存の署名つき文書に対する再処理の実施という5つを設定した．ここで



シーケンス	シーケンス発生確率 P_i	影響 M_i(コスト)	リスク $R_i = P_i \times M_i$	デジタル署名付文書の安全性確保
1	$P_1 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot (1-\bar{P}_5)$	M_1	$R_1 = P_1 \times M_1$	成功
2	$P_2 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot \bar{P}_5$	M_2	$R_2 = P_2 \times M_2$	失敗
3	$P_3 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot \bar{P}_4$	M_3	$R_3 = P_3 \times M_3$	失敗
4	$P_4 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot \bar{P}_3$	M_4	$R_4 = P_4 \times M_4$	失敗
5	$P_5 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot (1-\bar{P}_5)$	M_5	$R_5 = P_5 \times M_5$	成功
6	$P_6 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot \bar{P}_5$	M_6	$R_6 = P_6 \times M_6$	失敗
7	$P_7 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot \bar{P}_4$	M_7	$R_7 = P_7 \times M_7$	失敗
8	$P_8 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot \bar{P}_3$	M_8	$R_8 = P_8 \times M_8$	失敗
9	$P_9 = P_0 \cdot \bar{P}_1$	M_9	$R_9 = P_9 \times M_9$	失敗

図4　デジタル署名のイベントツリー

(d)の「署名つき文書の再処理を試みる」というのを入れたのは，署名者は通常自分にとって都合の悪いものに署名をするので，公開鍵暗号が危殆化し，電子文書が無効になるのは都合の悪いことではなく，再署名を試みないこともあるからである．

次に分岐について説明する．

(a) 最初の対策方法である暗号危殆化情報の確認機能が失敗してしまった場合，「暗号危殆化情報の伝達」は実施できないので，以降の分岐は存在しない．

(b) 暗号危殆化情報の伝達（署名者に伝達）に失敗しても，暗号危殆化情報の伝達（検証者に伝達）に成功すれば，「再処理を試みる」を実施し，以降の対策に成功すれば，デジタル署名付き文書の安全性確保に成功する場合も考えられるので，分岐が存在する．

(c) 暗号危殆化情報の伝達（検証者に伝達）に失敗した場合，「暗号危殆化情報伝達」（署名者に伝達）が成功しても，再署名などを実施したいのは検証者なので「再処理を試みる」ことなく，デジタル署名付き文書の安全性確保に失敗してしまう．したがって以降の分岐は存在しない．

(d) 既存の署名付き文書に対する再処理の実施を試みなければ，再処理の実施はないので以降の分岐は存在しない．

(3) 最適化問題としての定式化

本稿では，様々な具体的対策案の組合せが存在する中で，各種の対策コストを制約条件に置いたとき，トータルコストに関する目的関数を最小にする最適解を導き出す．

対策方法の採用方法としては前節で述べたように0-1変数を用いて表現する．対策方法を採用する時には変数 X に1を代入し，採用しない時には，X に0を代入する．ここでは，シーケンスごとの損害リスク値の和と各関与者の対策コストを加算したものをトータルコストとし，トータルコストが最小になるものを目的関数とする．定式化結果は式(1)に示すとおりである．

制約条件を政府の対策コスト，企業の対策コスト，署名者の対策コスト，検証者の対策コストとし，それら定式化したものが式(2)，(3)，(4)，(5)である．このあたりは各関与者の利害のバランスを取るために導入したものであり，いろいろな変形例が考えられる．

Minimize:

$$\sum_{l=1}^{L} R_l + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{gij} \cdot X_{ij} + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{cij} \cdot X_{ij} + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{sij} \cdot X_{ij} + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{vij} \cdot X_{ij} \quad (1)$$

$$(X_{ij}=0, 1 \sum_{j=1}^{J_i} X_{ij}=1 (i=1, 2, \cdots, I))$$

Subject to:

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{gij}\cdot X_{ij} \leq C_g \quad (2)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{cij}\cdot X_{ij} \leq C_c \quad (3)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{sij}\cdot X_{ij} \leq C_s \quad (4)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{vij}\cdot X_{ij} \leq C_v \quad (5)$$

ここで,

X_{ij}：対策案グループ i において j 番目の対策案を採用するかどうかを決定する変数

対策案 i-j を採用するなら $X_{ij}=1$，採用しないなら $X_{ij}=0$.

なお，$\sum_{j=1}^{J_i} X_{ij}=1$ は，対策案グループ i において採用しうる具体的対策案は必ず1つであることを表している．またここで，J_i は対策案グループ i における対策案の数である．

具体的には，次のような対策案を選定した．ここでは，後でも述べるように対策案グループをヘッディング項目ごとに設定している．

1．暗号危殆化情報の確認機構

(1-1) 監視機関なし (X_{11})

(1-2) CRYPTREC による監視 (X_{12})

(1-3) CRYPTREC による監視の強化 (X_{13})

2．暗号危殆化情報の署名者への伝達

(2-1) 伝達手段なし (X_{21})

(2-2) 既存の認証局による伝達 (X_{22})

(2-3) 新しく設置する伝達機関による伝達 (X_{23})

(2-4) 認証局と伝達機関による伝達 (X_{24})

3．暗号危殆化情報の検証者への伝達

(3-1) 伝達手段なし (X_{31})

(3-2) 既存の認証局による伝達 (X_{32})

(3-3) 新しく設置する伝達機関による伝達 (X_{33})

(3-4) 認証局と伝達機関による伝達 (X_{34})

4．署名付き文書の再処理を試みる

(4-1) 危殆化時対応ポリシーなし (X_{41})

(4-2) 危殆化時対応ポリシーあり (X_{42})

暗号が危殆化するのが分かったときに，署名者に強制的に再処理を行うようにさせるための契約などである．

5．既存の署名付き文書に対する再処理

(5-1) 対策なし (X_{51})

(5-2) 文書に対する再署名 (X_{52})

署名者に同じ文書に対し，強い公開鍵暗号で再度署名をしてもらうもの．

(5-3) 第三者機関による追加署名 (X_{53})

既存の署名付文書に対し，時刻認証局などの強い公開鍵暗号で追加署名してもらうものである．

I：対策案グループの総数．ここではヘッディング項目数と同じとなるように定式化している．

l：イベントツリーにおける l 番目のシーケンス

L：イベントツリー分析におけるシーケンスの総数

R_l：イベントツリーにおけるシーケンス l のリスクの値であり次のようにして求められる．

$$R_l=P_l\cdot M_l \quad (6)$$

M_l はイベントツリーにおけるシーケンス l の影響の大きさをあらわす．

$$P_l=P_0\cdot\prod_{i=1}^{H}\hat{P}_i \quad (7)$$

i は i 番目のヘディング項目をあらわす．

H はヘッディング項目数 I と同じ値になる．

$\hat{P}_i$ は i 番目のヘディング項目の分岐確率

$$\hat{P}_i=((1-\bar{P}_i)(1-y_i)+\bar{P}_i\cdot y_i) \quad (8)$$

$$y_i=\begin{cases}1：ヘッディング項目が下に展開\\0：ヘッディング項目が横に展開\end{cases}$$

ここで，式(7)は，P_l が，初期事象 P_0 と各ヘッディング項目の発生確率の積で表現できることを表している．また，式(8)に示すとおり，$\hat{P}_i$ は，各ヘッディング項目が，下に展開する場合と横に展開する場合のいずれの場合も対応できるように表現したものである．式(7)(8)より，例えば，シーケンス2の場合は，$P_2=P_0\cdot(1-\bar{P}_1)\cdot(1-\bar{P}_2)\cdot(1-\bar{P}_3)\cdot(1-\bar{P}_4)\cdot\bar{P}_5$ と表すことができる．

また，式(8)の $\bar{P}_i$ は以下のように定義される．

$$\bar{P}_i=\sum_{j=1}^{J_i} P_{ij}\cdot X_{ij} \quad (9)$$

ここでP_{ij}は，対策案 i-j を採用した場合のイベントツリーの下方への分岐確率を表している．すでに述べたように，ヘッディング項目別に対策案グループを設定するようにしている．また，$\sum_{j=1}^{J_i} X_{ij}=1$ であるので，対策案グループごとに1つの対策案が選ばれるようになっている．

C_{gij}：対策案 i-j を採用した場合の政府の対策コスト，ここでは，CRYPTREC の対策コストも政府の対策コストに含むことにした．

C_{cij}：対策案 i-j を採用した場合の企業の対策コスト，これは，認証局と時刻認証局などの第三者機関のコストである．

C_{sij}：対策案 i-j を採用した場合の署名者の対策コスト，

C_{vij}：対策案 i-j を採用した場合の政府の対策コスト，

C_g：政府の対策コストにおける制約値，

C_c：企業の対策コストにおける制約値，

C_s：署名者の対策コストにおける制約値，

C_v：検証者の対策コストにおける制約値，

このように定式化した後，各種パラメータの値を設定した．紙面の制約でパラメータの値はここには記述できないので必要に応じて文献[4]を参照願いたい．定式化とパラメータの設定が完了した後，多重リスクコミュニケータを用い危殆化対策の最適組合せを求めた．多重リスクコミュニケータでは，求解のために総当り法と辞書式枚挙法を実装しており，ここでは総当り法を用いた．

その結果をいろいろな専門家に見せつつ，合意が得られるまで，図1に示す過程を繰り返した．

4. 適用結果の考察

基本ケースにおける最適組合せは以下のとおりである[4]．

(1-3) CRYPTREC による監視の強化 (X_{13})

(2-1) 署名者への伝達手段は既存のまま (X_{21})

(3-3) 検証者への伝達は新しい伝達機関を設ける (X_{33})

(4-2) 署名者との間で危殆化時対応ポリシーあり (X_{42})

(5-3) 危殆化署名付文書へ第三者機関による追加署名 (X_{53})

この結果より次のようなことがいえる．

(a) CRYPTREC のような暗号監視機関の活動は重要であり，この活動を強化することが望ましい．

(b) 署名者に連絡する手段はすでにあるが検証者にはないので，暗号危殆化の情報を検証者に広く確実に伝達する仕組みが必要である．

(c) 暗号危殆化時には，電子借用書などの署名者が既存文書に再署名をしない可能性があるので，再署名ポリシーの事前締結などをして，再署名を確実にするよう強制するか，タイムスタンプ局で既存文書に自動追加署名する方式などを採用して強制しなくてもよい仕組みをつくるかの対応が不可欠である．

(d) タイムスタンプ局で既存文書に自動追加署名する方式のほうが，再署名ポリシーを事前締結して，署名を再作成するよりもトータルコストが小さくなる．

これらのうち，(b)(c)(d)については従来どこからも指摘されてこなかったものである．

5. おわりに

公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書の証拠性を確保するために必要な対策の最適な組合せを，費用とリスク低減効果のバランスを考慮しつつ求めることのできるリスク評価方法を提案するとともに，その一適用例を示した．その他のケースにおけるデジタル署名付文書への適用結果については，文献[4]を，長期署名フォーマット[7]というものへの適用結果については文献[6]を参照いただきたい．

今後は暗号が危殆化する前に対策が取れなかった場合についても検討していきたい．

参考文献

[1] 佐々木良一「IT リスクの考え方」岩波新書, 2008.

[2] 内閣官房情報セキュリティセンター “政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA 1024 に係る移行指針,” 2008 年 4 月 22 日, http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf.

[3] 三菱総合研究所 “暗号の危殆化に関する調査,” 情報処理振興機構, 2005 年 4 月. (http://www.ipa.go.jp/security/fy 16/reports/crypt_compromize/index.html).

[4] 藤本肇, 上田祐輔, 佐々木良一, “デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用,” 情報処理, Vol. 49, No. 3, pp. 1105-1118 (2008).

[5] 佐々木良一他, “多重リスクコミュニケータの開発と適用,” 情報処理学会論文誌 Vol. 49, No. 9, pp. 3180-3190 (2008).

[6] 西本敬志, 佐々木良一, “暗号危殆化に対する長期署名フォーマットの安全性評価,” 情報処理学会, CSS 2008 pp. 295-300.

[7] 次世代電子商取引推進協議会, “電子文書長期保存ハンドブック,” http://www.ecom.jp/results/h18seika/17_電子文書長期保存ハンドブック. pdf.